



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/050,274	01/16/2002	Yoon Seok Yang	2080-3-66	7037
35884 7590 01/04/2007 LEE, HONG, DEGERMAN, KANG & SCHMADEKA 801 S. FIGUEROA STREET 12TH FLOOR LOS ANGELES, CA 90017			EXAMINER BROWN, CHRISTOPHER J	
			ART UNIT 2134	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	
3 MONTHS			01/04/2007	
			DELIVERY MODE PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/050,274	Applicant(s) YANG, YOON SEOK	
	Examiner Christopher J. Brown	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 July 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

The request for continued examination has been accepted and reviewed.

Oath/Declaration

The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because: It does not identify the citizenship of each inventor.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 10, and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The applicant has repeated stated conversion of “block data” or “block units” to “byte data” or “byte units” and vice-versa. Even if the term “byte units” refers to the size of the unit, the terminology is indefinite because the term “block” can be interpreted as a “byte” and “byte” as a “block”. There is no relative difference in the two types of data as stated. Appropriate correction is required. Claims 2-9, 11-21, 23, and 24 are rejected for being dependent on the rejected independent claims.

Claim 10, rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The applicant states “carrying out a key schedule every round in response to a size and a key value” it is unclear what the “size and key value” are of, or what they refer to.

Claims 1, is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 states “outputting the converted block data of the byte units” this statement is difficult to understand. Since the claim already states “converting the received encrypted or decrypted block data into byte units,” the examiner recommends shortening the statement to “outputting the byte units”.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: encrypting or decrypting. The claim states “outputting the block data for encryption or decryption” and then “the control unit receiving encrypted or decrypted block data” but the claim does not state encrypting or decrypting..

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 4, 9-11, 14, and 21-23 rejected under 35 U.S.C. 102(b) as being anticipated by Wasilewski US 5,420,866 in view of Applied Cryptography, Bruce Schneier

As per claims 1, 10, and 22,

Wasilewski teaches a control unit receiving a data stream of byte units where the data stream is an MPEG data stream (encoder) (Col 8 lines 52-60, Col 9 lines 58).

Wasilewski does not explicitly teach converting data into block data for encryption.

Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12),

Schneier illustrates DES inherently uses 64 bit blocks (“Description of DES” pg 270).

Thus Wasilewski teaches that the MPEG stream must be converted into 64 bit blocks to be encrypted. Wasilewski teaches outputting encrypted stream data, thus the 64bit blocks of DES are converted from blocks back into bytes (Col 9 lines 30-36).

Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12),

Schneier illustrates that DES uses a key scheduling unit carrying out a key schedule every round in accordance with a size and key value of a block inputted so as to output a key value for the encryption or decryption of each round (“Outline of the Algorithm” page

270). Schneier illustrates the encryption process including receiving the key value from the key schedule unit so as to carry out encryption or decryption ("Decrypting DES" page 277). Thus Wasilewski teaches these items inherently by using the DES protocol

As per claim 2, Wasilewski teaches a control unit receiving a data stream of byte units where the data stream is an MPEG data stream (encoder) (Col 8 lines 52-60, Col 9 lines 58). Wasilewski does not explicitly teach converting data into block data for encryption. Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12), Schneier illustrates DES inherently uses a predetermined size of 64 bit blocks ("Description of DES" pg 270). Thus Wasilewski teaches that the MPEG stream must be converted into 64 bit blocks to be encrypted. Wasilewski teaches outputting encrypted stream data, thus the 64bit blocks of DES are converted from blocks back into bytes (Col 9 lines 30-36).

As per claim 4, and 14 Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12), Schneier illustrates that DES uses a key scheduling unit carrying out a key schedule every round in accordance with a size and key value of a block inputted so as to output a key value for the encryption or decryption of each round ("Outline of the Algorithm" page 270).

As per claims 9, and 21 Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12), Schneier illustrates that DES uses a key scheduling unit using a control signal to produce a key value every round in accordance with a size and key

Art Unit: 2134

value of a block inputted so as to output a key value for the encryption or decryption of each round ("Outline of the Algorithm" page 270).

As per claims 11, and 23 Wasilewski teaches the first format is a byte unit (MPEG stream) and the second format is a block unit (DES block), (Col 9 lines 8-15).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US 5,420,866 in view of Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000)

As per claim 12, Wasilewski teaches a control unit receiving a data stream of byte units where the data stream is an MPEG data stream (encoder) (Col 8 lines 52-60, Col 9 lines 58). Wasilewski does not explicitly teach converting data into block data for encryption. Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12), Schneier illustrates DES inherently uses a predetermined size of 64 bit blocks ("Description of DES" pg 270). Thus Wasilewski teaches that the MPEG stream must be converted into 64 bit blocks to be encrypted. Wasilewski teaches outputting encrypted

Art Unit: 2134

stream data, thus the 64bit blocks of DES are converted from blocks back into bytes (Col 9 lines 30-36). Wasilewski does not teach buffers.

Mroczkowski teaches data inputted from the control unit and then stores corresponding result in the output buffer of the control unit (Mroczkowski, section 2.1).

It would be obvious one of ordinary skill in the art to use the apparatus of Wasilewski with the protocol of Mroczkowski to provide an encryption scheme that is efficient for use with low-end microprocessors. .

As per claims 3, and 13 Wasilewski does not specify completeing all round calculations and storing the result in a corresponding output buffer. Mroczkowski teaches implementing a block cipher wherein a block round unit (Mroczkowski, Figures 1 and 2) completes all round calculation of data having been currently encrypted or decrypted before a next block data (Mroczkowski, input data) inputted from the control unit and then stores corresponding result in the output buffer of the control unit (Mroczkowski, section 2.1).

It would be obvious one of ordinary skill in the art to use the apparatus of Wasilewski with the protocol of Mroczkowski to provide an encryption scheme that is efficient for use with low-end microprocessors. .

Claims 5-8, 15-20, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US 5,420,866 in view of Daemen ("AES Proposal: Rijndael," March 1999),

As per claims 5-8, and 15-20, and 24 Wasilewski does not specify the inputted key value and size. Daemen teaches a key size of 128 bits (page 14 4.3) and an expansion algorithm for the Rijndael block cipher wherein the key expansion unit expands the inputted key value into a size amounting to $\{\text{block size} * (\text{count of rounds} + 1)\}$ (page 14, section 4.3.1) for the purpose of proposing a new encryption standard that is, among other things, efficient for use with 8-bit microprocessors (page 28, section 7.5). Daemen further teach that the key register has a capacity amounting to $\{(\text{size of an inputted block}) * (\text{size of one round})\}$ (Daemen, section 4.3.2). It is inherent that the key is stored in a key register.

It would be obvious one of ordinary skill in the art to use the apparatus of Wasilewski with the protocol of Daemen to provide an encryption scheme that is efficient for use with low-end microprocessors.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

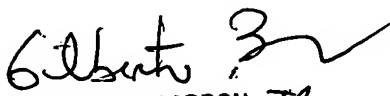
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jaques Louis Jaques can be reached on (571)272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown

9/30/06



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100